The Second European Recommendation concerning Payment Systems

Thunis, Xavier

Published in:
J.I.B.L.

Publication date:
1992

Document Version
Publisher's PDF, also known as Version of record

The Second European Recommendation Concerning Payment Systems: New Obligations for Card Issuers?

XAVIER THUNIS

Xavier Thunis, Deputy Director, Research Centre on Computer Law, Namur, Belgium

Introduction

The burgeoning of means of payment is without doubt one of the outstanding characteristics of what might be called the 'money' market. The traditional payment processes of notes and cheques have been joined by a multitude of instruments allowing people to settle their debts with varying degrees of deferment.

For the public as a whole, these financial innovations may be symbolised by a highly practical bit of plastic: the card. Or rather, cards, since there are many of them to suit all tastes: bank cards or store cards, credit cards or debit cards, even charge cards, track cards or smart cards.

This proliferation has its drawbacks if not controlled and kept in check. This is why there are now many initiatives, both legislative and 'para-legislative' (codes of conduct, recommendations, and so on) aimed at setting up a legal framework that is both flexible and equitable, and respects the interests of all parties involved.

At Community level, the recent initiatives reflect various concerns which are not always easy to reconcile.

Since it intends to place the development of new means[1] of payment within the context of financial and monetary integration for the Community, the Commission has manifested its desire to promote the interoperability of cards and, in general, the compatibility of the various payment systems in Europe.

In other words, both the efficiency and the universality of the payment systems are being targeted,[2] which implies close collaboration between the suppliers of payment systems, with all the risks of restricting competition which that can entail. There must therefore be an agreement on technical standardisation which will allow a system to be opened up to as many people as possible while respecting freedom of competition. Freedom of consumer choice is a mere illusion if the supply structure is not based on competition.

What is more, if they are not to be rejected, payment instruments can only be developed and distributed if the interests of all parties to the system – issuing institutions, traders and consumers – are respected. This was the theme of the two European recommendations of 8 December 1987[3] and 17 November 1988[4] concerning payment systems and in particular the relationship between card holder and card issuer. The second recommendation, which is the subject of our study, could largely be summarised by two key concepts: transparency and security.

In the belief that protection for the consumer, in the field of payment means, should be accelerated, the Commission considers that he ought to receive more complete and clearer information on the conditions – particularly financial ones – of the services provided. He also needs to have his liability limited in the event of the loss or theft of the means of access, and his rights asserted in the event that the issuer does not properly carry out the order it receives.

Legal form to be adopted: a recommendation

After many metamorphoses, the draft directive prepared by the Commission has finally become a recommendation, thus disappointing the consumer organisations which would have preferred a more binding text.[5]

It has been emphasised that a directive is too rigid an instrument, ill-suited to a subject characterised by rapid technical evolution. This carries the risk that legal provisions focused on a predetermined technical medium will become obsolete.[6] This is

1. The expressions, means and instrument of payment will be used indiscriminately although, strictly speaking, both the card and the cheque are merely *instruments* used for payment purposes.

2. See 'Tout atout pour l'Europe: les nouvelles cartes de paiement', COM(86)754 end; and more recently, 'Les paiements dans le marché intérieur européen', COM(90)447.

3. OJ 24 December 1987 L365/72, for a commentary, see M. Schauss, X. Thunis, 'Quelques réflexions à propos du code européen du bonne conduite en matière de paiement électronique', *DIT*, 1988/1, at 54 onward.

4. OJ 24 November 1988 L317/55.

5. On all the arguments used, see R. Trinquet, 'Les relations entre organismes financiers et consommateurs dans un système étendu à l'ensemble de la Communauté', *Banque* (Fr.), April 1989, at 424.

6. This is not a decisive argument since some states such as Denmark or the United States have not hesitated to pass legislation on the subject.

why a recommendation was chosen, since it ought to lead to an improvement in contractual conditions between issuer and holder.

Unquestionably, a directive which requires states to modify their internal law in accordance with its obligations is more restrictive than a recommendation.[7] But it should be noted that the recommendation, which except in one point is addressed to card issuers, also gives notice that they should modify the contractual provisions governing their relations with users. Issuers were given 12 months from the date of recommendation. Although issuers have not respected this deadline, it should be noted that, to avoid a directive, they had to adopt a code of conduct including many of the points contained in the recommendation. The code[8] and the recommendation will be compared frequently in the presentation below.

All the provisions in the recommendation—or, to be precise, its annex containing eight Articles—will not be examined in detail.

There will be a rapid description of the recommendation's scope (Chapter I) and the requirements it makes, concerning the agreement made between the issuer and the holder, of the means of access (contracting holder) (Chapter II).

However, attention will be focused on analysing the obligations of the holder (Chapter III) and the issuer (Chapter IV),, thereby highlighting the equilibrium being instituted between the partners and the new legal basis which underlies it (Chapter V).

Scope: Articles 1 and 2

The recommendation's scope is defined very broadly since it covers not only (point 1) all electronic payment or withdrawal operations made with or without a card, but also non-electronic payments by card:

> including processes for which a signature is required and a voucher is produced, but not including cards whose sole function is to guarantee payment made by cheque.

Operations initiated by card (payment, withdrawal, deposit) are covered very generally, whether the card is issued by a banking institution (see point 2 which explicitly covers the store card), whether the operations are initiated electronically, and whether the card is a debit, credit or charge[9] card.

The text even extends to 'electronic payment effected by a member of the public without the use of a card, such as home banking', which might seem premature given the lack of concrete experience in this last subject.

Emphasis has justly been placed on the imprecise or excessively broad scope of the recommendation.[10] The notion of payment is not mentioned anywhere else, and nor are 'connected operations' (does this refer to getting statements from the electronic terminal?). As for cards excluded from the scope of the recommendation, those 'whose sole function is to guarantee a payment made by cheque' – Eurocheque cards for example – these very often prove to be used for other functions (withdrawal or electronic transfer), in which case they would come under the recommendation.[11]

There are other difficulties of interpretation. It has been asked whether the text covered and protected not only consumers but also undertakings. It must be concluded from both the letter and the spirit of the text that it excludes transactions carried out by a professional in the course of his business as well as those initiated by an undertaking within the context of a tele-banking contract concluded with its financial institution. What is sought here is protection for the individual consumer wishing to satisfy his own needs.[12]

7. See Article 189 of the Treaty; however, one should be wary of making simplistic contrasts and should consider that a recommendation has no legal authenticity. Nevertheless, in a decree of 13 December 1989 (JLMB 1990, at 326 onward), the Court of Justice of the European Communities emphasised that the acts in question cannot thereby be considered totally without legal effect. Indeed, national judges are bound to take account of the recommendations in order to solve disputes submitted to them. The court of Juvisy sur Orge did in fact do just that in an unpublished decision of 27 April 1990; the court stated explicitly that the unsolicited sending of a card to a customer is contrary to the recommendation and the code of conduct adopted by the profession.

8. The exact title is, 'Code of best practice of the European banking industry on card-based payment systems'. It constitutes the reply of the European Credit Sector Associations to the Commission's recommendation. For an explanation of the contents of the code, see D. Iannucci, 'Le code de bonne conduite du secteur bancaire européen concernant les systèmes de paiement par cartes', AEBDF September 1991.

9. Even though some of these cards do not allow the customer's bank account to be directly debited without another payment instrument also being used (withdrawal advice or cheque), see R. Trinquet, Note 5, at 426.

10. See in particular the pertinent questions raised by G. Nicolas, 'La recommandation de la Commissions des Communautés européenes du 17 novembre 1988 concernant les systèmes de paiement', *Banque et Droit* 3, March/April 1989, at 68; R.E. van Esch, 'De aanbeveling van de Europese Commissie inzake betalingssystemen', *Computerrecht* 1989/2, at 95 onward.

11. In this respect, see Y. Gérard and A. Svendsen, 'La recommandation de la Commission sur les relations entre organismes financiers et porteurs de cartes de paiement', *DIT*, 1989/2, at 51 onward.

12. Because of this, 'company cards' issued to a legal person and used by its employees within the context of their jobs may be excluded from the scope of the recommendation. In this respect, see E. Meysmans, 'Aanbeveling van de EG-Commissie van 17 november 1988 inzake betalingssystemen en met name inzake de betrekkingen tussen de kaarthouder en de verstrekker van de kaart', *Doc. KB*, at 5.

These difficulties of interpretation,[13] some of which are already resolved in the European banking sector's code of conduct concerning card-based payment systems, should probably not be exaggerated. The code of conduct excludes home banking, and deals with the bank payment cards (credit and debit) used by private individuals on their own account.

Nevertheless, the absence of an overall approach at the Community level is to be deplored in a subject as important as that of payment. Thus, the very broad scope of the 1988 Recommendation does not coincide with the much more restrictive one defined by the Recommendation of 8 December 1987 which covers only electronic payment and excludes store cards and card payments made by mechanical procedures.

It is also regrettable that no serious studies were carried out beforehand on the apportionment of risk as concerns cheques or bank transfers, which would surely have thrown up useful information on the subject of cards.

The Agreement between the Issuer and the Holder of Means of Access (Contracting Holder)

There now follows a rapid review of the requirements imposed by the recommendation as concerns the form of contract, its conclusion and modification. The obligations of the contracting parties are examined in a separate section below.

Form and wording of the contract: Articles 3.1 and 3.2

Article 3.1 of the recommendation indicates that:

> Each issuer shall draw up full and fair terms of contract in writing, to govern the issuing and use of the payment devices he issues.

The requirement for a written document is evidence of the renaissance of a degree of 'formalised protection' which would lead to a new variety of solemn contract.[14]

The clauses must be *fair*, this being a notion borrowed from 'Anglo Saxon' law[15] which might call to mind the general principle of good faith in contractual relations.

They must also be *complete*, a requirement which in practice is not easy to comply with given the evolution and multiplicity of the services offered. In any case, it should be understood that the principal elements of the contract must be included in the document[16] and that no plea can be raised against clauses which are simply referred to.[17] The clauses must also be 'expressed in easily understandable words and in so clear a form that they are easy to read.'.[18]

Finally, the clauses must be worded,

> in the language or languages which are ordinarily used for such or similar purposes in the regions where the terms of contract are offered.

This complicated formulation doubtless means that the agreement has to be drawn up in the official language(s) of the place of conclusion. Practice in Belgium is along these lines.

The obligation of issuers to specify the financial conditions of the service offered to the contracting holder will be discussed later in this article.

Conclusion of the contract: Article 5

Article 5 contains two series of stipulations. According to the first:

> the contract between the issuer and the contracting holder shall be regarded as having been concluded at a time when the applicant receives the payment device and a copy of the terms of contract accepted by him.

For the contract to be formed, the payment instrument has to have been supplied to the holder. Could this be a new form of actual contract?[19] Whatever the case, it is in the interest of issuers to arrange for proof of delivery of the card and contractual conditions if they wish to collect their dues and avail themselves of contractual stipulations applying, for example, in the event of the loss or theft of the means of access.[20]

The second stipulation is that, 'No payment device shall be dispatched to a member of the public except in response to an application from such

13. For a critical commentary of the definitions given under point 2, particularly the notion of a system provider, see also R.E. van Esch, Note 10, at 86 and the example cited; G. Nicolas, Note 10, at 68.
14. See M. Schauss and X. Thunis, Note 3; also, R. Trinquet, Note 5, at 425.
15. See G. Nicolas, Note 10, at 69; for a comparison between English and French law, see D. Harris and D. Tallon (eds.), *Contract Law Today*, Clarendon Press, 1989.
16. See G. Nicolas, Note 10, at 69; E. Meysmans, Note 12, at 9.
17. See Y. Gérard and A. Svendsen, Note 11, at 51.
18. This provision has sometimes been criticised because of its vague and imprecise nature – see G. Nicolas, Note 10, at 59; this criticism seems rather harsh. The necessary degree of legal precision in a contract must not be abandoned. But both the presentation and the wording of the contract must allow the 'average' customer to understand the scope of the undertakings being subscribed to.
19. See above the notion of solemn contract, see also G. Nicolas, Note 10, at 69; Y. Gérard and A. Svendsen, Note 11, at 52.
20. See on this subject the precedent cited by X. Thunis and M. Schauss, 'Aspects juridiques du paiement par carte', *Cahiers du CRID*, 1, Story Scientia 1988, at 27 onward (a case of misuse before the consumer received the means of access).

person.' This prohibition which can be found in Danish (Article 14.1) and American (EFTA, Article 903.1) regulations aims to put an end to the practice of sending unsolicited cards. It should, however, be understood that such a provision does not apply in the case of card renewal.[21] The code of conduct (point 8) stipulates explicitly:

> The card issuer shall not dispatch a card to a customer unsolicited, except where the card is a replacement for a card already held by the customer.

Modification of contract: Article 3.5

The basic legal principle mentioned in the recommendation is that, 'the terms of contract shall not be altered except by agreement between the parties.' However, the recommendation relaxes its requirements when it indicates that:

> . . . however, such agreement shall be deemed to exist where the issuer proposes an amendment to the contract terms and the contracting holder, having received notice thereof, continues to make use of the payment device.

This flexibility is desired by issuers and is based on the fact that the silence in question is accompanied by active behaviour on the part of the holder who, by using the card, is deemed to adhere to the new conditions which are communicated to him.

How, by what means? Is a simple letter sufficient, given the number of holders concerned? A notice in bank premises is possible but runs the risk of raising problems concerning proof that the holder has been informed.

If the customer refuses the modification, he has the opportunity to terminate the contract and return his card. From the issuers' point of view, it seems advisable to insert a clause in the contract specifying how modifications are to be brought to the contracting party's knowledge, and also to provide that, after a certain period, the holder is deemed to have accepted the proposed modifications.[22] In this respect, point 5 of the code of conduct indicates:

> sufficient notice of the change shall be given to the card holder to enable him to withdraw if he so chooses. A period shall be specified after which time the card holder would be deemed to have accepted the terms if he had not previously withdrawn.

21. See in this respect the extremely detailed provisions of the EFTA (Electronic Fund Transfer Act), particularly Article 911(b) according to which, means of access may be sent in the absence of a request. But the conditions are very strict.

22. In this respect, see Y. Gérard and A. Svendsen, Note 11, at 52; see also, the recommendations made by the Conseil National de Crédit (France) in its reports of July 1986 and March 1988 in favour of a concerted procedure for reviewing contracts.

The Obligations of the Contracting Holder

The recommendation places a number of obligations on the holder, intended to prevent payment mishaps or to limit their consequences. So it is true that the holder himself must contribute also to the security of payments and the instruments by which they are made.

Safety of the payment instrument: Article 4.1(a) and (c)

The holder has an obligation of prudence. This is specified explicitly by the recommendation which obliges him to:

> take all reasonable steps to keep safe the payment device and the means (such as a personal identification number or code) which enable it to be used.

For example, this forbids him to leave his card in a place where it could easily be used (in a car, for example). As is shown by past case law on cheques, not all cases are easy to settle. What about a card left in an office or else in a handbag left for a moment on a shop counter?

It is sure that writing the confidential code on the means of payment or any other document carried with the latter is a common form of negligence: but borderline cases can arise. What about the code number noted in a list of telephone numbers, 'embedded' if appropriate in the midst of dummy numbers?

As will be seen, it is very important to be able to qualify the behaviour of the interested party since 'extreme negligence' aggravates the holder's liability (see below).

One could ponder about the safety obligation imposed on the customer and the consequences of default. Can it be inferred from fraudulent use of the card by a third party that, somehow or other, the holder has passed on his access number to a third party, thereby committing extreme negligence which deprives him of the limitation of liability provided by the recommendation (see below).

Obligation to make opposition: Article 4.1(b)

The holder must:

> notify the issuer or a central agency, without undue delay after becoming aware:
> - of the loss or theft or copying of the payment device or of the means which enable it to be used;
> - of the recording on the contracting holder's account of any unauthorised transaction;

– of any error or other irregularity in the maintaining of that account by the issuer.

More detailed coverage will be given to the obligation of notification in the case of loss or theft of the card. The last two hypotheses refer to the holder's obligation to consult his statements of account and react in the event that an irregularity is discovered on reading them. This obligation will become all the more intense when, after automation, transfers take place quickly and the customer's collaboration is required so that irregularities affecting the conduct of his account can be rectified. The procedure for rectifying errors (error resolution procedure) set up by the American EFTA may be seen in this light.[23] The aim of this procedure is to allow errors affecting the customer's account to be rectified as quickly as possible *without* legal action.[24] An account holder who has not reacted within 60 days as from receipt of the statements of account forfeits either the benefit of automatic rectification or even, in some cases, the benefit of liability limitation instituted by law.

It is indisputable that, in the case of dispossession of the means of access, the holder must demonstrate diligence; he must make opposition, that is, tell the issuer of the loss or theft of his card and his code.

The recommendation is not very specific on the circumstances in which opposition is to be made. No form is imposed: written opposition duly received by the issuer is preferable in order to avoid any dispute as to the time of opposition.[25] According to the recommendation, opposition must be made without undue delay after dispossession is discovered. This provision obviously creates difficulties. How is excessive delay to be judged? In particular, its starting-point is left to the total discretion of the holder. If he is negligent or if he simply does not use his payment instruments very often, he is likely to take some time to notice their disappearance. Proof of when the loss was discovered, which is admittedly pivotal in apportioning liability (see below) is likely to prove very difficult for the issuer.

Irrevocability of the payment order: Article 4.1(d)

Like the French law of 11 July 1985 (Article 22) and the recommendation of 8 December 1987, the recommendation of 17 November 1988 obliges the holder not to revoke a payment order which he himself has issued.

This explicit provision satisfies both issuers and traders, both anxious to keep the payment transaction separate from the underlying commercial transaction and not to put the security of payments at issue.[26]

This seems in line with the technical evolution in payment instruments. Since it brings closer together the time that the order is issued and the time it is executed, it tends in practice to make it difficult to revoke.

Obligations of the Issuer: Articles 3.3, 3.4, 4.3, 6[27]

Obligation of confidentiality

> The terms of contract shall put issuer under obligation *vis-à-vis* the contracting holder not to disclose the contracting holder's personal identification number or code or similar confidential data, if any, except to the contracting holder himself.
> (Article 4.3).

It is worth asking what is meant by this rather vague expression – information relating to payment mishaps which the card holder has already experienced and would be taken up on the latter?

Obligation of information: Articles 3.3 and 3.4

The issuer must specify in the contract the financial conditions of the service provided, namely:

> (1) the basis for calculating the amount of charges (including interest) – an obligation which, it seems, raises tricky practical problems;[28]
> (2) the period within which transactions are entered on the account (immediate or deferred debit) as well as invoicing by transaction.

Proof of transactions: Article 6

As frequently underlined, the traditional principles governing the law of proof give pre-eminence to a signed written document (Article 1341 of the French Civil Code). There are, however, exceptions in the

23. EFTA, Article 908.
24. For a broad view of settlement procedures, see N. Lheureux and L. Langevin, 'La pratique des cartes de paiement au Québec: Rapport de droit comparé', *Revue du Barreau* (Canada), March/April 1990, at 271 onward.
25. Judicial practice in France is particularly strict in this respect; see recently Cass. fr. (ch. com.) 23 June 1987, *DIT*, 1988/3, at 38 onward, note by J. Huet; in practice, other processes are known for receiving oppositions given by telephone. A case number is given to the opposing customer, which allows him to prove the time of opposition.
26. M. Vasseur, in 'Le paiement électronique. Aspects juridiques', *JCP* 1985, I, 3206 no. 12, underlines that irrevocability is pregnant with meaning, since it dissociates the payment instrument from the commercial transaction.
27. The issuer's obligations regarding opposition will be examined later.
28. For further details, see G. Nicolas, Note 10, at 70; E. Meysmans, Note 12, at 11 onward.

law itself (see Articles 1347 and 1348) which will not be analysed here.[29] Derogations in agreements are also possible, but within certain limits (see below). So the problem is not, in this matter, to escape the pre-eminence of written proof, but to tap into modern techniques for elements which are reliable and can if possible be cross-checked, such that presumptions may be drawn from them as to the existence and content of the transaction as well as the identity of the parties thereto.

With the introduction of automated techniques, it can be observed that a sort of *'obligation of proof'* is emerging for which the issuers of payment instruments are responsible.

As all elements of proof are concentrated with the issuer and the depersonalisation of transactions makes it difficult to prove a precise fact directly (for example the disclosure of a code), there is a stress on the security conditions that have to surround the production and preservation of documents. This trend was already emerging in the Council of Europe's recommendation of 11 December 1981 (R(81)20), relating to the admissibility conditions for reproductions of documents and computer entries. This emerges in Article 6.1 of the European recommendation, according to which:

> issuers shall keep, or cause to be kept, internal records which are sufficiently substantial to enable operations to be traced and errors to be rectified.

And also, it could be added, to constitute sufficiently reliable presumptions which are likely to attract the judge's support in the event of conflict over the identity of the issuer of the order, and over the existence or amount of the transaction (see below).

This is not enough to restore the traditionally required bilateral nature to the elements of proof. Unless he himself can take part in producing the proof, the contracting holder must at the very least be able to exercise some control over the way in which transactions are recorded, so that he can pick up anomalies and promptly ask for them to be rectified.

Hence the requirement is made on issuers during a contract, to meet their obligation of information by issuing sufficiently precise and complete documentation to users. This documentation may in practice take two forms: the slip issued when the transaction takes place, or the statement of account subsequently setting out a series of transactions with references by which they can be identified. In Article 6.3, the recommendation seems to cover both possibilities by indicating:

> The contracting holder, if he so requests, shall be supplied with a record of each of his operations, instantaneously or shortly after he has completed it . . .

This requirement for information can also be found in recent legislation such as the American Electronic Fund Transfer Act (EFTA). This obliges banks to supply regular and extremely detailed documentation[30] both at the actual transaction site and subsequently in the form of a periodic summary. Apart from informing the customer – namely, the American consumer – this document is very significant in determining his rights.

The American consumer forfeits the benefit of the error resolution procedure if he does not notify the irregularity within 60 days from receipt of a periodical statement of account.

The user's obligation of vigilance and diligence could even be sanctioned by increased liability[31] if it proves that the absence of consultation has meant that fraudulent debits have been aggravated.

As concerns current Belgian banking practice, the conclusive force of various information media produced at the time of the transaction is carefully specified. Thus, there is a provision that:

> documents (slips) issued by the cash dispenser or point-of-sale terminal do not constitute proof of the transaction but are only supplied to the card holder for information or to allow him to make a check.

In contrast:

> the journal strip or an equivalent information medium, on which the details of operations carried out at each cash dispenser or point-of-sale terminal are recorded, constitutes a binding and sufficient process of proof in writing.

French and Belgian doctrine and judicial practice[32] accept without too many reservations the validity of agreements on proof, even though these do not seem to be able to prevent a party from providing contrary proof[33] (see also below).

29. There is an abundant bibliography. For a summary, see X. Thunis and M. Schauss, Note 20, at 43 onward; M. Fontaine, 'La preuve des actes juridiques et les techniques nouvelles', *La Preuve*, UCL 1987. In France, see in particular F. Gallouedec-Genuys, *Nouvelles technologies de l'information et droit de la preuve*, La documentation française, Paris, 1990.

30. For further details, see in particular EFTA Article 906.

31. EFTA Article 909; compare, in Belgian judicial practice, Comm. Liège, 19 January 1984, *Dr. Inform.*, 1984/2, at 29 onward.

32. It has been considered in Belgian judicial practice that the journal strip constituted adequate proof for two withdrawals made 10 days apart, Trib. civ. Namur, 30 May 1988, *DIT*, 1990/2, at 60 onward, note by J.P. Buyle; in France, Cass. fr. (1st ch.), 8 November 1989, *DIT*, 1990/2, at 44 onward, note by Vasseur.

33. In this respect, see J. Huet, 'Formalisme et preuve en informatique et télématique', *Informatique et télécommunications: y a-t-il un juriste dans la salle?* Story Scientia 1989, at 242 onward; see also, for the Netherlands, Article 6.5.2 A3 of the NBW sanctioning the clause, *dat de bevoegheid van de wederpartij om bewijs te leveren uitsluit of beperkt.*

Finally, as concerns statements of account, Belgian bank regulations contain clauses according to which operations shown on statements are deemed to have been approved by the customer unless he protests to the bank within a certain period (60 days or even 30 days).

The validity of such clauses is under discussion.[34] Is it usual for the passage of time to lead by agreement to an irregularity being ratified and the holder being deprived of his rights to the amounts due to him?

According to Article 1315 of the French Civil Code, the *burden of proof* falls on whoever claims the performance of an obligation. Anyone who claims to be released must provide evidence either of payment, or of the fact that has led to his obligation being extinguished.

Going beyond the wording of these important principles, modern doctrine stresses collaboration between the parties in establishing proof.[35] It should also be emphasised that the burden of proof reacts to rights actually acknowledged for the issuer on the one hand, and the 'contracting holder' on the other hand, in the event of the theft or loss of the card (and in general the means of access) (see below for examples).

On the basis of the imbalance between the parties in producing and controlling the elements of proof, in other words, the 'greater aptitude for proof' of the issuing establishment, Article 6.2 of the recommendation obliges the issuer, in the event of conflict over liability relating to an unauthorised electronic funds transfer, to:

> show that the operation was accurately recorded and accurately entered into accounts and was not affected by technical breakdown or other deficiency.

This type of provision, which can be found in American legislation,[36] imposes a very onerous task on the issuer. This torrent of proofs, some of which are negative, would be impossible to retrieve[37] unless the issuer is authorised to demonstrate that the system as a whole operated satisfactorily during the period in question.[38] In the event of dispute, the debate then moves on to the reliability of the system in place. If an assessment of the system's reliability proves negative, the issuer has to provide direct proof of the customer's imprudence, which is very difficult to establish unless the customer admits it or the card, or some other document on which the customer has noted his code number, is recovered.

But current judicial practice (see below) seems to consider that the systems are safe and that it is highly unlikely that disfunction of the system could lead to debits in favour of a third party guilty of fraud with no fault on the customer's part, that is, without the secret code being communicated. In theory, reversing the burden of proof seems favourable to the user; in practice, the issuing institution will more often than not be able to produce elements of proof whose admissibility and conclusive force have been contractually enshrined (see above) and on the basis of which the judge will conclude that the equipment was not defective at the time it was used by the holder (no irregularity noted during the period around the withdrawal, internal checking mechanisms, and so on.)[39] The holder will then have to prove specific default, which will not be easy. Reversing the burden of proof is therefore not a panacea if all the elements of proof likely to sway the judge's conviction are concentrated in the hands of the same party.

In two cases submitted before the Geschillencommissie (Netherlands),[40] the customer disputed having made withdrawals which the bank wished to charge to him. The card had remained in his possession and, at the time of the withdrawals, he was either at his place of work or at home. If the customer was to be believed, there must have been fraudulent withdrawals made by a third party who had neither the card nor the code. As for the bank, it produced records showing that the customer's means of access had definitely been used. According to the commission, the customer's assertion, however probable, that he could not have been at the withdrawal location did not constitute sufficient contrary proof. He had to prove that it was impossible for a third party to have had access to the code and the card in order to carry out the disputed withdrawals. This judicial precedent, however, is not definitively fixed. Some decisions have shown greater clemency to the holder of the means of access.[41]

In France, having shown doubts as to the reliability of systems,[42] judicial practice now seems to be postulating that the systems are reliable and

34. See H. Croze, Notes on Cass. fr. (ch. com.), 9 December 1986, *JCP* 1988, II, 20918 no. 2 onward; J. Vézian, *La responsabilité du banquier en droit privé français*, Librairies Techniques, 1983, at 51 no. 77.

35. See in particular N. Verheyden, 'La charge de la preuve', *La Preuve*, UCL 1987, at 5 and the many references cited.

36. See EFTA, Article 909 B.

37. In this respect, see G. Nicolas, Note 10, at 70.

38. See Y. Gérard and A. Svendsen, Note 11, at 54; M. Vasseur note to Cass. fr. (ch. civ.), 8 November 1989, *DIT*, 1990/2, at 47 onward; see also point 15 at the end of the code of conduct:

> . . . The correct recording of previous and subsequent similar transactions shall constitute *prima facie* evidence that the system was functioning properly.

39. For a case of application, see the Tribunal d'instance of Nuremberg, 15 October 1976, *Rev. europ. dr. cons.*, 1987, at 382.

40. See Geschillencommissie Bankbedrijf, 21 October 1987, *Computerrecht* 1988/3, at 152 onward, note by Stuurman; Geschillencommissie Bankbedrijf, 17 May 1988, *Computerrecht* 1989/1, at 39 onward.

41. See Geschillencommissie Bankbedrijf, 24 April 1990, *Computerrecht* 1990/4, at 201 onward, and note by Ch. Knobbout-Bethlem.

42. Paris, 1 December 1980, *Dr. Inform.*, 1986/3, at 124.

cannot operate without a confidential code. Any use by a third party guilty of fraud after the theft or loss of the card, can then only arise from the holder being faulty in guarding his secret code.[43]

It is difficult to foresee the extent to which the recommendation challenges judicial practice as mentioned above. However, the question of whether the holder's fault (passing on the code) must be proved or can be presumed remains just as important, since the limitations of liability established by the recommendation do not apply in the case of the holder's 'extreme negligence' (see below).

Apportionment of Liability in the Event of a Payment Mishap

One of the most important aspects of the recommendation concerns the apportionment of liability between the issuer and the holder in the event of a payment mishap.[44]

Two hypotheses may be distinguished: non-performance or incorrect performance of an order given by the holder; and, the misuse of the means of access by a third party guilty of fraud following their loss or theft.

The recommendation contains important but sometimes rather unclear provisions[45] for settling these two hypotheses.

Non-performance or incorrect performance of the operations: Article 7

According to Article 7.1, the issuer is liable in the event of the non-performance or defective performance of operations, even when they are initiated using electronic equipment over which the issuer has no direct or exclusive control. It is also liable in the event of operations not authorised by the customer.[46]

Although this is not mentioned explicitly in the text, it should be understood that the issuer's liability is only involved for operations while they are being executed.[47] Otherwise, issuers would be held liable for any defect in their terminals (for example system breakdown, shortage of notes, etc.) duly noted by the user even *before* initiating the operation, which is not reasonable.[48] It could, however, be held that the issuing institution (or the group representing it) is obliged to bring a faulty machine back into operation as quickly as possible. Has not the introduction of automated systems made issuers responsible for a certain degree of *continuity* in providing the service?

Whatever the case may be, the recommendation contains an extremely onerous obligation on issuers, who are bound by defects in equipment over which they have no direct or exclusive control.[49]

Rather more than liability based on fault, this is a liability based on *risk* which in this case is ascribed to issuers. On the basis of Article 7.1, they are liable to the holder for incorrect execution resulting in:

> (1) defects in telecommunications networks (the plural is acceptable insofar as international transfers, which are increasingly frequent, involve the collaboration of several carriers which benefit from varying degrees of exoneration);
> (2) defects in equipment in the care of shopkeepers;
> (3) defects in equipment installed by foreign, competing issuers with which standardisation agreements have been made in order to encourage the international distribution of the payment system.[50]

In a frequently cited study,[51] M. Vasseur emphasises that the banker, in his capacity as a 'professional, is liable for his technique . . . he assumes the risk for it'. The recommendation goes even further. It is not only *his* technique for which the banker (issuer) is liable: he is also liable to the holder for the technique *of others*, that is, third institutions with which he

43. Pau, 17 October 1984, *Dr. Inform.*, 1986/3, at 126; Douai, 26 October 1983, *Dr. Inform.*, 1986/3, at 121; Paris, 29 March 1985, *Dr. Inform.*, 1988/3, at 122. Might this judicial practice be in the process of evolution? See the decision of the Versailles Court of Appeal of 21 December 1990 (*INC*, Hebdo 731, 21 June 1991) according to which the fault of the card holder must be mentioned. It should also be stated that in this case the bank committed several errors (sending out the opposition late, incomplete files, etc.) which may have influenced the decision. See also Cass. (ch. com.) 8 October 1991, D.S. 1991 at 583 onward.

44. The term 'payment mishap' is used to describe any event affecting a transfer or withdrawal order, the object or effect of which is to cause a delay or modification in its issuing or execution.

45. See on this point the critiques of G. Nicolas, Note 10, at 70 onward; Y. Gérard and A. Svendsen, Note 11, at 55; R.E. van Esch, Note 10, at 100.

46. The hypothesis covered could be queried, since Article 8 also covers in detail the case of unauthorised operations following the loss or theft of the means of access. In the opinion of the author, this must refer to an operation carried out by the issuer without an order from the holder, regardless of any fraud by a third party.

47. In this respect, see Y. Gérard and A. Svendsen, Note 11, at 55.

48. In the United States, Article 910 of the EFTA does explicitly provide:

> A financial institution shall not be liable . . . if the financial institution shows by a preponderance of the evidence that its action or failure to act resulted from . . . a technical malfunction which was known to the consumer at the time he attempted to initiate an electronic fund transfer. . . .

49. Article 13 of the code of conduct does indeed seem to diverge from the recommendation in this respect since it indicates that, 'the issuer shall be liable for direct losses incurred by a card holder due to a system malfunction directly within the issuer's control.'

50. It is regrettable that a degree of imprecision in the recommendation means that liability for equipment installed in the home by the holder for what are known as 'home banking' operations cannot be excluded.

51. *JCP*, 1985, no 38.

has made an agreement so that the payment system is distributed nationally and internationally. This is a quite remarkable phenomenon.

Article 7.2 limits the issuer's responsibility:

> (1) to the amount of the operation in the case of non-performance or defective performance;
> (2) to the sum necessary to put the customer back in his previous position in the case of an unauthorised operation.

This limitation of responsibility, even if it is toned down by Article 7.3,[52] is interesting.

The development of systems based on risk can go hand in hand with the fixing of ceilings of liability for the party bearing the risk, namely the issuer. However, should the issuer, as a result of its grave negligence or intentional fault, cause the giver of an order a loss which is irreparable by the fixed amounts provided, then the latter could have recourse to ordinary law and go through the system provided by it (proven fault, discussion on the link between causality and the foreseeable or unforeseeable nature of the loss, etc.).

Liability in the event of loss or theft of the card: Article 8

The apportionment of liability in the case of loss or theft of the means of access is one of the most important and also most frequently discussed points of the recommendation. To get a good understanding of the scope of the change made by it, the apportionment of liability in the Belgian system currently being adapted will briefly be examined.

Belgian system: apportionment of liability in electronic payment matters

In Belgium, contracts made between banks and their customers for orders given at terminals installed in public places rest (rested) on the following system: the account holder bears the full risk for operations carried out after theft, loss or misuse of the means of access, until he tells the bank (issuer) about the illicit operations or the risk of illicit operations.

The holder's liability ceases as soon as he has told his bank and the latter has (within a reasonable time) been able to take the necessary measures to prevent any subsequent fraudulent use. In outline, this system was common to the three sets of 'regulations' governing the use of electronic payment cards in Belgium (Mister Cash, Bancontact, Postomat).

52. Article 7.3 provides that, other financial consequences, particularly as concerns the extent of loss for which compensation must be paid, are governed by the law applicable to the contract concluded between the issuer and the contracting holder.

It is necessary to underline the importance of opposition in this system, since it produces a swing in the burden of risk. Before the theft is notified, the holder has *unlimited* liability for financial losses linked to the misuse of the card. Once the loss or theft is notified and the reasonable time necessary to intervene has elapsed, further loss is caused by the negligence of a bank (or service company) which does not take adequate security measures.

Belgian case law,[53] which is fairly sparse, has accepted this sharing out of liability by agreement while making the following additions:

> (1) Once opposition has been notified, the bank's obligation of prevention is an *obligation of result*. It must immediately take the necessary measures and may not delay them because of considerations of opportuneness.
> (2) The bank has *full* liability for fraudulent withdrawals after the customer's opposition, even if the customer has previously committed a fault such as disclosing the secret code to a third person.[54]
> (3) The issuer is obliged to set up a permanent system for receiving oppositions, even at weekends and on public holidays. The absence of such a system constitutes a design fault for which the issuer must bear all prejudicial consequences, irrespective of the customer's fault.[55]

The system set up by the recommendation: Article 8

Notification is an essential element in the apportionment of liability provided for by the recommendation. Article 8.1 does explicitly provide that:

> Each issuer shall provide means whereby his customers may at any time of the day or night notify the loss, theft or copying of their payment devices . . .

This text is an effective expression of 'the obligation of security' imposed on issuers by reason of the systems they offer the public.

As in the Belgian system, notification is the starting-point for the *sharing* of liability. Except in cases of 'extreme negligence' or fraud, the customer is no longer liable from the moment when he notifies the issuer (or a central agency) (Article 8.2).

53. For a full summary, see X. Thunis and M. Schauss, Note 20, at 33 onward.
54. On the first two points, see Trib. comm. Liège 1984, *Dr. Inform.*, 1984/2, at 298, Liège, 22 February 1985, *Dr. Inform.*, 1985/3, at 28. Reservations have generally been made on these two decisions on the part of Belgian doctrine, which advocates a sharing of liability conforming more to the theory or equivalence of conditions which is generally accepted in Belgian law.
55. In this respect, see J.P. Verviers, 23 November 1984 and Court of First Instance Vervier, 8 January 1986, *DIT*, 1988/3, at 58 onward and critical note by M. Schauss.

Losses suffered before notification are charged to the contracting holder, 'up to the equivalent of 150 ecus for each event, except where he has acted with extreme negligence or fraudulently' (Article 8.3).

The system provided has a few remarkable characteristics. The most notable difference from the Belgian system is unquestionably the limitation of liability from which the holder benefits *before notification of loss or theft*. But this limitation gives way in the event of extreme negligence or fraud. The constitution of this extreme negligence is not defined in the recommendation. Does it have to be proved by the issuer or can it be presumed?

The case most frequently mentioned is the holder's violation of his obligation of prudence which, in particular, compels him not to write down the confidential code on the payment means or any other document kept with it (Article 4.1(c)). Violation of this obligation certainly constitutes extreme negligence. The question is then, whether this has to be proved by the issuer or whether it can be presumed as from the moment when the operation of the system implies that the third party guilty of fraud knows the secret code. Taking the second alternative, limitation of liability could prove somewhat theoretical. Other cases of extreme negligence may be envisaged, for example, late notification (but here too, there is the question of how one establishes the time by which the holder should discover the loss or theft) or else late consultation of statements meaning that the loss is aggravated (what about a holder on holiday or abroad?).

The second notable difference is that *after notification of the loss or theft*,[56] the contracting holder is no longer liable except, once again, for extreme negligence or fraud (Article 8.2). The role of this latter exception could damage the holder's situation more than in the Belgian system (see above). The principle established by Article 8.2 – immediate release of the holder as from notification – is difficult to reconcile with Article 8.4 which seems to impose only an obligation of means and not of result on the issuer.[57] Even if it does *everything*, the issuer might not manage to prevent the fraudulent use of the means of payment. Time is needed to broadcast an international opposition, a case of *force majeure* might prevent the blocking measures from being implemented.[58] Who is going to bear the prejudicial consequences of fraud between the time of notification and the time when an issuer of normal diligence and conscientiousness is able to give an effective result? According to the recommendation, in principle it is the issuer who bears the risk. Legally, its obligation exceeds the obligation of result and is close to an obligation of guarantee.[59]

Reflections on the evolution of the basis of liability in payment systems

Whereas judicial practice in Belgium and France on cheques and bank transfers is characterised by a casuistic approach based on the respective fault of the banker and the holder, it seems that as concerns automated payment, particularly cards, this approach tends to become somewhat blurred.

As early as the law of 1 March 1961, as concerns cheques, the Belgian legislator, to a large extent, broke with the concept of fault by asserting that the holder should bear the risks of misuse of the cheque and may be debited by the amount of a false or falsified cheque unless the banker has committed fraud or gross negligence.

Such a solution is based on the *risk created* by the holder who is in a better position than the banker to prevent its occurrence. This basis is also what seems to underlie the apportionment by agreement of liability in Belgian 'regulations' prior to the recommendation. Before opposition, it is the holder who bears the unlimited burden of risk because he is most likely to be able to prevent its occurrence; after opposition, it is the issuer who has or should have a system responding effectively to notifications of loss or theft.

With the European recommendation of 17 November 1988, a basic evolution has taken place. The holder's liability *before* opposition is limited, which is a total reversal compared with the previous solution. In principle, liability falls to the issuer because it is more capable, not necessarily of preventing the occurrence of loss, but of absorbing its financial consequences by distributing them. This is not the basis of control of the created risk but that of profit-risk which explains the best similar solution. It is most unlikely that this is the end of fault. Whether created risk or profit-risk, or a combination of the two, is paramount, fault emerges once again with – paradoxically – perhaps a heightened moral attribute insofar as unacceptable behaviour by one of the parties, either the holder or issuer, leads to the ceilings of liability being eliminated or increased.

Professor Viney[60] once showed that the development of a more collective system of reparation based on risk goes hand in hand with a 'counter-offensive of culpability'. The subject of payments does seem to provide a remarkable illustration of this phenomenon.

56. Not as from the moment when the issuer has, within a reasonable period, been able to take the necessary preventive measures.
57. See R. Trinquet, Note 5, at 428.
58. On these two examples, see E. Meysmans, Note 12, at 48.
59. The issuer of the means of access is therefore obliged to set up a permanent system of opposition having (in practice) immediate effect.
60. G. Viney, 'Le déclin de la responsabilité individuelle', LGDJ, 1965.